UNIVERSITY of NICOSIA

Course Syllabus

Course Code	Course Title	ECTS Credits
COMP-359	Data Privacy	6
Prerequisites	**Department**	**Semester**
COMP-211, MATH-225	Computer Science	Spring
Type of Course	**Field**	**Language of Instruction**
Elective	Computer Science	English
Level of Course	**Lecturer(s)**	**Year of Study**
1st Cycle	Dr Ioanna Dionysiou	3rd
Mode of Delivery	**Work Placement**	**Corequisites**
Face-to-face	N/A	None

Course Objectives:

The main objectives of the course are to:

- examine privacy threats such as pervasive surveillance, profiling, location analysis, and traffic analysis
- present privacy-by-design concept and principles
- provide students with deep knowledge on state-of-the-art privacy enhancing techniques
- present the problem of computing on data such as homomorphic encryption, secure multi-party computation, statistical disclosure control and techniques based on differential privacy
- examine the legal context of privacy such as legislations and directives (e.g. general data protection regulation GDPR)
- discuss privacy issues and challenges in various application domains
- explore cutting-edge research topics in privacy.

Learning Outcomes:

After completion of the course students are expected to be able to:

1. explain the privacy threats in network systems and services
2. discuss and explain current privacy enhancing techniques to mitigate privacy threats and risks
3. discuss differential privacy properties and mechanisms
4. discuss trade-offs between quality of protection and cost, bandwidth and latency in anonymous communications

5. perform a long-term traffic analysis attack
6. analyze the privacy challenges for a given application domain
7. discuss the privacy requirements as expressed in legislations such as the GDPR

Course Content:

1. Motivation for privacy
2. Engineering privacy, including privacy and data protection principles from legal frameworks
3. Privacy-by-design strategies
4. Contemporary privacy enhancing techniques in protocols and storage
    a. privacy features of authentication protocols
    b. secure private communications
    c. communications anonymity and pseudonymity
    d. privacy in databases
    e. storage privacy
5. Contemporary privacy enhancing techniques for
    a. respondent privacy
    b. owner privacy
    c. user privacy
6. Privacy-preserving computations via homomorphic encryption, secure multi-party computation and differential privacy
7. Social, economic and legal context of privacy protection, privacy policies and standard privacy practices
8. Legal frameworks for privacy, including GDPR
9. Data privacy in various application domains such as biomedics, social networks, etc.

Learning Activities and Teaching Methods:

Lecture, Individual Work and Case Studies.

Assessment Methods:

Final Exam, Midterm Exam, Assignments and Semester Project.

Required Textbooks / Readings:

Title	Author(s)	Publisher	Year	ISBN
The Algorithmic Foundations of Differential Privacy	C. Dwork and A. Roth	Now Publishers Inc	2014	978-1601988188

(Foundations and Trends in Theoretical Computer Science)				
Privacy and Data Protection by Design – from policy to engineering	George Danezis, Josep Domingo-Ferrer, Marit Hansen, Jaap-Henk Hoepman, Daniel Le Métayer, Rodica Tirtea, Stefan Schiffner	European Union Agency for Network and Information Security	2014	978-92-9204-108-3

Recommended Textbooks / Readings:

Title	**Author(s)**	**Publisher**	**Year**	**ISBN**
Data Privacy Law: A Practical Guide (2nd edition)	G.E. Kennedy and L.S.P. Prabhu	Interstice	2017	978-0999512715

Due to the nature of the course, most of the reading assignments will be from original research papers.